Japanese Unexamined Patent Application Publication No. 2002-215826

SPECIFICATION <EXCERPT>

[0005] The present invention has been devised in view of the above problems, and an object of the present invention is to provide a certificate automatic updating apparatus that automatically updates a certificate in which information necessary for updating certificate is included, when the certificate is soon to be expired or has already been expired.

****

[0007] A certificate automatic updating apparatus including: a storage device which stores a certificate and a certificate update program that automatically updates the certificate by connecting to a server computer with a certificate authority function; an application program that uses the certificate; and a client computer which connects to the server computer immediately before expiration of the certificate or after the expiration of the certificate and requests automatic update of the certificate, wherein the certificate includes a certificate update program activating unit which activates expiration information and the certificate update program, and the certificate automatic updating apparatus receives and stores an updated certificate in the storage device while connecting to the server computer immediately before the expiration of the certificate or after the expiration of the certificate and requesting the automatic update of the certificate.

****

[0011] FIG. 4 shows an example of information that the certificate authority records in the certificate 101. A start date of a valid period of the certificate 101 is denoted by 400. An end date of a valid period of the certificate 101 is denoted by 401. Certificate authority address information is denoted by 402. The certificate

authority address information 402 depends on a connection specification to the certificate authority 105, and may be a URL or IP address. A certificate update program name for connecting to the certificate authority 105 by referring to the certificate authority address information 402 and updating the certificate 101 is denoted by 403, and specifies the certificate update program 102, for example. A certificate update program activating unit for actually activating the certificate update program 102 is denoted by 404. When the application 103 accesses the certificate 101, the certificate update program activating unit initially operates. A certificate update program start procedure which shows a procedure for activating the certificate update program 102 is denoted by 405. An automatic update start parameter which specifies how many days before the end date of the valid period 401 the automatic update of the certificate is performed is denoted by 406.

[0012] FIG. 5 shows an example of a general sequence of the certificate automatic updating apparatus. A user 500 performs starting 501 on the application 103. When the application 103 is started, access 502 to the certificate 101 necessary for coding, signing, and so on is performed. A storage destination of the certificate 101 is one of the hard disk of the client computer 100, the IC card 201, and the removal medium 301 such as a floppy disk.

****

[0014] When the certificate update program 102 is activated, connection 505 to the certificate authority 105 via a network is performed according to the certificate authority address information 402 of the certificate 101. Subsequently, the certificate update program 102 sends a certificate update request 506 to the certificate authority 105. When the certificate authority 105 receives the certificate update request 506, the certificate authority 105 sends an update process request 507 to the certificate update program 102, so as to obtain information necessary for actually

updating certificate. The certificate update program 102 which has received the update process request 507 sends an update process request 508 to the user 500, so as to obtain information necessary for updating certificate from the user 500.

[0015] The user 500 who has received the update process request 508 performs input 509 of the information necessary for updating certificate. The certificate update program 102 returns an update process reply 510 to the certificate authority 105 based on the information inputted by the input 509. The certificate authority 105 which has received the update process reply 510 performs issuance of certificate 511 for the certificate update program 102 according to the update process reply 510. The certificate update program 102 which has received an updated certificate performs storage of certificate 512 in one of the hard disk, the IC card 201, and the removable medium 301 such as the floppy disk. Subsequently, the certificate update program 102 notifies the user 500 of completion of certificate update 513 indicating that the certificate update process has been successful and performs return 514 of control to the application 103. This allows the certificate to be updated by automatically connecting to the certificate authority 105, even when the user 500 is not aware of the connection to the certificate authority 105. Thus, the user can continue the application 103 performing processes without paying attention to an end date of a valid period 401 of the certificate 101.

[0016] FIG. 6 is a flow chart showing a certificate automatic update process flow. Here, it is assumed that the application 103 has already been started. First, in step 600, the application 103 accesses the certificate. In step 601, the certificate update program starting unit 404 stored in the certificate 101 is started. The certificate update program activating unit 204 reads an automatic update start parameter in step 602 and obtains a current time in step 603.

[0017] In step 604, the obtained current time and the end date of the valid period 401 stored in the certificate 101 are compared. When the certificate has been expired, the flow proceeds to step 606, and when the certificate has not been expired, the flow proceeds to step 605. In step 605, a start date of automatic update is determined by subtracting the number of days specified with the automatic update start parameter 406 from the end date of the valid period 401, and the determined start date and the current time are compared. When the determined start date has been reached, the flow proceeds to step 606, and when the determined start date has not been reached, the process is finished. In step 606, the certificate update program name, the start procedure, and the certificate authority address are read. In step 607, the certificate update program activating unit 204 activates the certificate update program based on the read information. The activated certificate update program 102 connects to the certificate authority 105 via the network, and performs the certificate update through, for instance, the sequence shown in FIG. 5. When the certificate authority 105 issues an updated certificate in step 609, the process is finished by receiving and storing the updated certificate on a recording medium. It is to be noted that a storage destination may be the recording medium on which a certificate before update is stored.

[0018] FIG. 7 is a flow chart when deleting an old certificate before update after the certificate is automatically updated. Here, it is assumed that the certificate 101 is soon to be expired or has already been expired, and that automatic update is to be performed. First, the certificate automatic update is performed, as described in detail by FIGS. 5 and 6, in step 700. In step 701, an updated certificate is received from the certificate authority 105, and the received certificate is stored. In step 702, a dialogue message is displayed to ask the user whether or not the certificate before update is to be deleted. When the user inputs a response for

deletion, the flow proceeds to step 703, and when the user does not input the response for deletion, the process is finished. The certificate before update is deleted in step 703. This prevents the old certificate from consuming memory of the recording medium.

[0019] FIG. 8 is an overall block diagram when certificate authorities exist and each of the certificate authorities issues a certificate. A server computer A is denoted by 800. A certificate authority A included in the server computer A 800 is denoted by 801. A server computer B is denoted by 802. A certificate authority B included in the server computer B 800 is denoted by 803. A certificate that is issued by the certificate authority A 801 and stored in a hard disk of a client computer 100 is denoted by 804. Likewise, a certificate issued by the certificate authority B 803 is denoted by 805. Even when the certificate authorities exist, an updated certificate can be received from each of the certificate authorities with the same procedure as in the above-mentioned case where there is the single certificate authority.

[0020] FIG. 9 is a flow chart showing a certificate automatic update process flow in the structure shown in FIG. 8. Here, it is assumed that the certificate A 804 and the certificate B 805 are soon to be expired or have already been expired, and that automatic update is to be performed. First, in step 900, the application 103 accesses the certificate A. In step 901, the certificate update program starting unit 404 reads a certificate update program name, a start procedure, and an address of the certificate authority A. In step 902, a certificate update program is activated based on the read information. In step 903, the activated certificate update program 102 performs the certificate update with the certificate authority A. In step 904, when the certificate authority A801 issues an updated certificate, the updated certificate is received and stored.

[0021] In step 905, the application 103 accesses the certificate B.

In step 906, the certificate update program starting unit 404 reads a certificate update program name, a start procedure, and an address of the certificate authority B. In step 907, a certificate update program is started based on the read information. In step 908, the started certificate update program 102 performs the certificate update with the certificate authority B. In step 909, when the certificate authority B 801 issues an updated certificate, the updated certificate is received and stored.

[0022] As stated above, the automatic update of the certificates A 804 and B 805 that are respectively issued by the certificate authorities A 801 and B 803 is completed. This enables the automatic update of certificate even with a structure which includes certificate authorities and in which a certificate issued by each of the certificate authorities is used.

[0023] As described above, when the certificate in which information necessary for updating certificate is included is soon to be expired or has already been expired, the certificate is updated by automatically connecting to the certificate authority. Thus, even if the user does not become aware of a valid period of a certificate or connecting to the certificate authority that is a certificate issuing authority, the user who works using an application that ensures security using the certificate can automatically connect to the certificate authority, update the certificate, and return control to the application when the application accesses the certificate, when the certificate is soon to be expired or has already expired. For this reason, the user is less bothered by the suspension of the application, restart, and so on; saved from searching the address of the certificate authority to be used for issuing a certificate and URL; and can prevent the suspension of the work caused by not updating the certificate. Further, the above-mentioned automatic update can be implemented in every application which can use the certificate without specific alterations. This makes it easier to

ensure the user to perform the certificate update.

DRAWINGS

図４　証明書情報例: FIG. 4 Example of certificate information

101: Certificate

400: Start date of valid period

401: End date of valid period

402: Certificate authority address information

403: Certificate update program name

404: Certificate update program activating unit

405: Certificate update program start procedure

406: Automatic update start parameter

図５　証明書自動更新シーケンス: FIG. 5 Certificate automatic update sequence

101: Certificate

102: Certificate update program

103: Application

500: User

501: Starting

502: Access

503: Start

504: Return

505: Connection

506: Certificate update request

507: Update process request

508: Update process request

509: Update process input

510: Update process reply

511: Issuance of certificate

512: Storage of certificate
513: Completion of certificate update
514: Return
期限間近または失効: Soon to be expired or already expired

図６　証明書自動更新の流れ図: FIG. 6 Flow chart of certificate automatic update
証明書自動更新: Certificate automatic update
600: Access to certificate
601: Start certificate update program activating unit
602: Read automatic update start parameter
603: Obtain current time
604: Certificate already expired?
605: Start date of automatic update reached?
606: Read certificate program name, start procedure, and address of certificate authority
607: Activate certificate update program
608: Certificate update process with certificate authority
609: Store updated certificate
終了: End

図７　更新前証明書削除の流れ図: FIG. 7 Flow chart showing deletion of certificate before update
更新前証明書削除: Deletion of certificate before update
700: Automatically update certificate
701: Store updated certificate
702: Delete certificate before update?
703: Delete certificate before update
終了: End

図８　認証局と証明書が複数の構成の場合: FIG. 8 Case where structure includes certificate authorities and certificates

100: Client computer
102: Certificate update program
103: Application
800: Server computer A
801: Certificate authority A
802: Server computer B
803: Certificate authority B
804: Certificate A
805: Certificate B

図９　認証局と証明書が複数の場合の証明書自動更新の流れ図: FIG. 9 Flow chart of certificate automatic update when certificate authorities and certificates exist
証明書自動更新（複数構成）: Certificate automatic update (structure including certificate authorities and certificates)
900: Access to certificate A
901: Read certificate program name, start procedure, and address of certificate authority A
902: Activate certificate update program
903: Certificate update process with certificate authority A
904: Store updated certificate
905: Access to certificate B
906: Read certificate program name, start procedure, and address of certificate authority B
907: Activate certificate update program
908: Certificate update process with certificate authority B
909: Store updated certificate
終了: End